REMARKS

Applicant respectfully requests reconsideration of this application as amended. Claims 1, 17 and 25 have been amended. Claims 4, 10-16, 20-24 and 28 were cancelled without prejudice. No new claims have been added. Therefore, claims 1-3, 5-9, 17-19, 25-27 and 29-30 are presented for examination.

35 U.S.C. § 112 Rejection

Claims 1-3, 5-9, 17-19, 25-27 and 29-30 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirements.

Claims 1, 17 and 25 have been amended. Accordingly, Applicants respectfully request the withdrawal of the rejection of claims 1, 17 and 25 and their dependent claims.

35 U.S.C. § 103 Rejection

Claims 1-3, 5-9, 17-19, 25-27 and 29-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas, Jr., et al., U.S. Patent No. 6,687,375 ("Matyas") in view of Dole, et al., U.S. Patent No. 6,628,786 ("Dole") in view of Hardy, et al., U.S. Patent No. 6,073,242 ("Hardy") in view of Menezes, et al. "Handbook of Applied Cryptography", ("Menezes") and further in view of Bening, et al. U.S. Patent No. 6,061,819, ("Bening").

Claim 1, as amended, recites:

> A method comprising:
> initializing a pseudo-random number generator (PRNG);
> obtaining local seeding information from a host;
> securely obtaining remote seeding information from remote entropy servers via a secure entropy collection protocol, the secure entropy protocol relying on unpredictable random numbers, each of the remote entropy servers having a random state machine generating

the remote seeding information, the remote seeding information to be mixed with the local seeding information to provide an unpredictable system status to amplify entropy to enhance system security, wherein the remote seeding information is to facilitate unpredictability of the unpredictable system status, wherein the enhancing of the system security includes securing an initial seed state via the remote entropy servers;

repeating the securely obtaining of the remote seeding information for each entropy server;

generating a key pair including a temporary asymmetric public key and a temporary asymmetric private key;

encrypting the temporary public key with a public key associated with a remote entropy server;

decrypting the temporary public key with a private key associated with the remote entropy server;

encrypting the remote seeding information with the temporary public key;

decrypting the remote seeding information with the temporary private key; and

stirring the PRNG via the local seeding information and the remote seeding information.

(emphasis supplied)

Applicants respectfully disagree with the Examiner's characterization of the pending claims and the cited references. Applicants maintain that the Examiner's assertion that "Chen et al teaches obtaining seeding information from a remote entropy server" is incorrect. (Chen's col. 1 lines 66- col. 2 lines 9). Applicants respectfully submit that Chen does not do so. *There is no reference to the word "remote" or obtaining seeding information from a "remote" entropy server.* (col. 1 lines 66- col. 2 lines 9).

Applicants respectfully disagree with the Examiner's characterization of the references and Response to Arguments even when the cited references are "considered as a whole." (Office Action, mailed 10-11-06, pages 6-7) However, for the sake of expediting issuance of this case, Applicants provide additional remarks for the Examiner's consideration.

Matyas discloses a "computer program which generate[s] a cryptographic key utilizing user specific information to generate a user dependent key." (Abstract). Matyas

further discloses "*a PRNG . . . for generating pseudo random numbers. [T]he PRNG having only one secret seed value.*" (col. 9, lines 19-25; emphasis added). Chen discloses "[a] method . . . for *communicating encrypted user passwords from a client to a server.*" (Abstract; emphasis added). Chen further discloses that "[t]he server *communicates to the client a server random seed value.* The client then *generates a client random seed value* and, using both the client random seed value and the server random seed value, an encrypted user password. The client then *communicates to the server the client random seed and the encrypted user password.* Then the server validates the encrypted user password using both the server random seed and the client random seed." (col. 2, lines 1-9; emphasis added).

Hardy discloses "[a]n electronic communication authority server that provides centralized key management, implementation of role-based enterprise policies and workflow and projection of corporate authorities over trusted networks." (Abstract). Hardy further discloses that "*a secure connection is a connection where the level of confidentiality, authentication, and integrity is sufficient* for the purposes of the system owners and users." (col. 3, lines 54-56; emphasis added). Menezes discloses that "a session key is an ephemeral secret, i.e., one whose use is restricted to a short time period such as a single telecommunications connection, after which all trace of it is eliminated." (page 494, lines 3-5).

Bening discloses an "inventive mechanism generates reproducible random initial states for use in simulation testing a design of a logic machine. The mechanism uses the hierarchical path names for the modules of the design and a random seed to generate reproducible random initialization states. Since the path names and the seed are known quantities, the random number can be reproduced. This allows the logic designs to be tested by different simulation methods and still have the same initialization states.

Furthermore, if the simulation fails, design changes can be verified by using the same initialization states which caused the failure." (emphasis supplied)

Claim 1, as amended, in pertinent part, recites "securely obtaining remote seeding information from remote entropy servers via a secure entropy collection protocol, **the secure entropy protocol relying on unpredictable random numbers, each of the remote entropy servers having a random state machine generating the remote seeding information**, the **remote seeding information to be mixed with the local seeding information to provide an unpredictable system status to amplify entropy to enhance system security**, wherein **the remote seeding information is to facilitate unpredictability of the unpredictable system status, wherein the enhancing of the system security includes securing an initial seed state via the remote entropy servers**" (emphasis added). Matyas, Chen, Hardy, Manezes, and Bening, neither individually nor when combined in any combination, teach or reasonably suggest at least these features of claim 1. Accordingly, Applicants respectfully request he withdrawal of the rejection of claim 1 and its dependent claims.

Claims 17 and 25 contain limitations similar to those of claim 1. Accordingly, Applicants respectfully request he withdrawal of the rejection of claims 17 and 25 and their dependent claims.

Conclusion

In light of the foregoing, reconsideration and allowance of the claims is hereby earnestly requested.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Request for an Extension of Time

Applicant respectfully petitions for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: January 9, 2008

Aslam A. Jaffery
Reg. No. 51,841

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980